NETWORK INTRUSION DETECTION AN ANALYST'S HANDBOOK

By Stephen Northcutt, Judy Novak and Donald McLachlan
SAMS, 2000, Second Edition. ISBN: 0-7357-1008-2.

The need for intrusion detection analysis continues to grow. This book is training aid and reference for intrusion detection analysis. It is based on the authors' experience in training and certification of intrusion analysts and the formal training curriculum, developed over the years. The second edition adds material that will help the reader to learn intrusion detection and to prepare for certification. For those who are willing to put the effort to become truly skilled at intrusion detection, it not only provides the knowledge, but also the structure for an accelerated learning curve.

The handbook is written by three authors with diverse experience. Stephen Northcutt is author of several books including *Incident Handling Step by Step* and *Intrusion Detection-Shadow Style*, as well as contributing editor for *Securing NT Step by Step* published by the SANS Institute. He was the original author of the Shadow intrusion detection system and leader of the Department of Defense's Shadow Intrusion Detection Team before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. He serves as the lead incident handler for the Global Incident Analysis Center and Director of Training and Certification for the SANS Institute. Judy Novak is senior security analyst at the Johns Hopkins University Applied Physics Laboratory. She is involved in information assurance and research and development for the APL enterprise network. She worked for three years on the Army Research Labs Computer and Incident Response Team. Donald McLachlan' main strength is in systems and network programming in C on Unix and various real time operating systems. This strength is coupled with experience in designing and implementing link layer protocols for HF network data communications systems, as well as with long experience with computer system security.

COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION

Historically each nation and multi-national organization established its own set of computer security evaluation criteria. Examples included the UK, Canadian, U.S. and European Union security evaluation criteria. Although these evaluation criteria were similar in scope and adequate for their own unique environments, they were, in fact, different in detail. These differences resulted in developers of trusted products having to subject their products to separate evaluations by each nation or multi-national organization. There was no mutual recognition of evaluations among the nations and this quickly became an impediment to the development of trusted products because it fragmented the market into too many pieces thereby reducing the economic incentive for the developers—it became too costly and took too long to get approval of trusted products. Realizing this problem would only worsen over time, the nations agreed in the spring of 1993 to develop a set of Common Criteria, which would replace the ITSEC, CTCPEC, TCSEC, FC and others. The nations indicated above have signed up to participate in the development and subsequent use of the Common Criteria. A great deal of progress has been made since 1993 and the first and second versions of the CC were released in January 1996 and January 1998 respectively. The Common Criteria and related efforts now form a common basis for developing and evaluating trusted products in the U.S., Canada, the European Union, NATO and other nations. It is already facilitating the mutual recognition of evaluations and thereby broadening the availability of trusted products for all participants.

The Common Criteria (CC) provide a framework for the development of protection profiles, which are the mechanism used to specify the user's security requirements in an implementation independent manner. Based on the protection profile developers can then develop a security target that is a detailed statement of the security features that they will provide to meet the protection profile. The security target is usually specific for each implementation and includes the assurance requirements that the developer intends to meet. The CC also provides a set of predefined assurance packages, referred to as Evaluation Assurance Levels (EALs), which are based to some extent on existing evaluation criteria—e.g., the Trusted Computer Security

Evaluation Criteria (TCSEC). International Mutual Recognition Agreements for EALs 1 through 3 have already been agreed between the US, CA, and the UK. Development of Protection Profiles is underway and several already exist for C2 and B1 systems and firewalls. Security Targets have also been submitted by developers for firewalls, routers and some applications.

TCSEC

Trusted Computer System Evaluation Criteria (TCSEC), known as Orange Book, are published in august 1983 by National Computer Security Centre (NCSC), a part of National Security Agency (NSA). They define the basic classes and trusted computer system evaluation criteria.

The Orange Book defines four broad hierarchical divisions of security protection. In increasing order of trust, they are:

- D - minimal security;
- C - discretionary protection;
- B - mandatory protection;
- A - verified protection.

Each division consists of one or more numbered classes, with higher numbers indicating a greater degree of security.

Although many of the concepts and mechanisms described in the Orange Book are applicable to network environment, the Orange Book doesn't define what's needed to make a network secure. Concerns about the security of data transmitted over communications networks led to the development of standard criteria for evaluating the level of trust that can be placed in a computer network. In an effort to extend the TCSEC evaluation classes to trusted network system and components, NCSC published the Trusted Network Interpretation of the Trusted Computer Evaluation Criteria (TNI, the Red Book) in 1987. Like The Orange Book , the Red Book describes broad security principles. Because network evaluation is still so ill defined when viewed from perspective of actual system in complex network environment, the Red Book requirements are likely to be revised in the near future.

ITSEC

Information Technology Security Evaluation Criteria (ITSEC, published by the Federal Republic of Germany in 1992), defines a standard that's under development for international security. The ITSEC, which have become known as "Europe's White Book" defines classes of functionality and assurance levels.

COMMON CRITERIA

ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of international standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote. International Standard ISO/IEC 15408 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information Technology, in collaboration with the Common Criteria Implementation Board, a joint entity composed of members of the Common Criteria Project Sponsoring Organizations. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organizations as Common Criteria for Information Technology Security Evaluation, version 2.0.

The seven governmental organizations collectively called “the Common Criteria Project Sponsoring Organizations” are:

- Communications Security Establishment, Canada
- Service Central de la Sécurité des Systèmes d'Information, France
- Bundesamt für Sicherheit in der Informationstechnik, Germany
- Netherlands National Communications Security Agency, The Netherlands
- Communications-Electronics Security Group, United Kingdom
- National Institute of Standards and Technology, United States
- National Security Agency, United States

The version 2.1 of the Common Criteria for Information Technology Security Evaluation (CC 2.1) is a revision that aligns it with International Standard ISO/IEC 15408:1999. In addition, the document has been formatted to facilitate its use. Security specifications written using this document, and IT products/systems shown to be compliant with such specifications, are considered to be ISO/IEC 15408:1999 compliant. CC 2.0 was issued in May, 1998. Subsequently, a Mutual Recognition Arrangement was established to use the CC as the basis of mutual recognition of evaluation results performed by the signatory organisations. ISO/IEC JTC 1 adopted CC 2.0 with minor, mostly editorial modifications in June, 1999.

CC version 2.1 consists of the following parts:

- Part 1: Introduction and general model;
- Part 2: Security functional requirements;
- Part 3: Security assurance requirements.

The Common Criteria project

Sponsoring organizations

GERMANY:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
German Information Security Agency (GISA)
Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany
Tel: +49.228.9582.300, Fax: +49.228.9582.427
E-mail: cc@bsi.de
WWW: http://www.bsi.bund.de/cc

NETHERLANDS:
Netherlands National Communications Security Agency
P.O. Box 20061
NL 2500 EB The Hague
The Netherlands
Tel: +31.70.3485637, Fax: +31.70.3486503
E-mail: criteria@nlncsa.minbuza.nl
WWW: http://www.tno.nl/instit/fel/refs/cc.html

UNITED KINGDOM:
Communications-Electronics Security Group
Compusec Evaluation Methodology
P.O. Box 144
Cheltenham GL52 5UE
United Kingdom
Tel: +44.1242.221.491 ext. 5257, Fax: +44.1242.252.291
E-mail: criteria@cesg.gov.uk
WWW: http://www.cesg.gov.uk/cchtml
FTP: ftp://ftp.cesg.gov.uk/pub

UNITED STATES - NIST:
National Institute of Standards and Technology
Computer Security Division
820 Diamond, MS: NN426
Gaithersburg, Maryland 20899
USA
Tel: +1.301.975.2934, Fax: +1.301.948.0279
E-mail: criteria@nist.gov
WWW: http://csrc.nist.gov/cc

UNITED STATES - NSA:
National Security Agency
Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 20755-6740
USA
Tel: +1.410.859.4458, Fax: +1.410.684.7512
E-mail: common_criteria@radium.ncsc.mil
WWW: http://www.radium.ncsc.mil/tpep/

NETWORK SECURITY ROADMAP

www.sansstore.org

Organizations

- Hewlett Packard – www.hp.com
- Hiverworld (Enterprise network security) – www.hiverworld.com
- Internet Security System – www.iss.com
- NetSecure Software – www.netsecuresoftware.com
- Network-1 Security Solutions, Inc – www.network-1.com
- ODS networks – www.ods.com
- Surf CONTROL – www.surfCONTROL.com
- TRIPWIRE Security Systems, Inc. – www.tripwiresecurity.com

White Papers

www.sans.org/tools.htm

Some consolidated information security vulnerabilities

- http://cve.mitre.org
- www.iss.net
- http://seclab.cs.ucdavis.edu
- www.cs.purdue.edu/coast/projects/vdb.html
- www.rootshell.com

Public domain security tools

- ftp://ciac.llni.gov/pub/ciac/sectools/unix/
- ftp://coast.cs.purdue.edu/pub/tools/
- ftp://ftp.cert.org/pub/tools/
- ftp://ftp.porcupine.org/pub/security/index.html
- ftp://ftp.funet.fi/pub/unix/security

Incident response centers

- www.auscert.org.au/
- www.cert.org/
- www.ciac.llnl.gov/
- www.assist.mil
- www.fedcirc.gov
- www.first.org
- www.cert.dfn.de/eng/dfncert/
- www.nasairc.nasa.gov/incidents.html
- www.fbi.gov/nipc/index.htm
- www.fbi.gov/contact/fo/fo.htm
- www.cert.dfn.de/eng/csir/europe/certs.htm

Good security web sites

- www.cerias.purdue.edu/coast
- www.telstra.com.au/info/security.htm
- www.nsi.org/compsec.htm
- www.securityportal.com/
- www.tne.nl/instit/fo/intern/wkinfsec.htm
- java.sun.com/security/
- www.ntbugtrag.com/
- www.boran.com/security/
- www.icsa.net/
- IOpht.com/
- ftp.porcupine.org/pub/security/index.htm

Government security web sites

- www.itpolicy.gsa.gov/
- www.cit.nih.gov/security.html
- www.nswc.navy.mil/ISSEC
- cs-www.ncsl.nis.gov/

Underground security web sites

- www.pharck.com/
- www.2600.com/

Some good security books

- www.amazon.com/
- www.clbooks.com/
- www.barnesandnoble.com/

Books

- Actually Useful Internet Security Techniques by Larry J. Hughes Jr.
- Applied Cryptography: Protocols, Algorithms and Source Code in C by Bruce Schneier
- Building Internet Firewalls by Brent Chapman & Elizabeth D. Zwicky
- Cisco IOS Network Security by Cisco Systems
- Designing Network Security by Mike Kaeo
- Firewalls and Internet Security by Bill Cheswick & Steve Bellovin
- Halting the Hacker: A Practical Guide To Computer Security by Dorothy E. Denning
- Internet Security for Buisness by Gene Shultz, et al
- Instruction Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response by Edward G. Amoroso
- Instruction Detection: Network Security Beyond the Firewall by Terry Escamilla
- Securing Java: Getting down to buisness with mobile code by Gary McGraw and Ed Felten
- Linux Security by John S. Flowers
- NT 4 Security by Michel Moncur, Charles Perkins and Matthew Strebe
- Network Intrusion Detection by Simson Garfinkel
- Practical UNIX and Internet Security, 2nd Edition by Simson Garfinkel & Gene Spafford
- The NCSA Guide to Enterprise Security: Protecting Information Assets by Michel E. Kabay
- Virtual Private Networks, 2nd Edition by Charlie Scott, Paul Wolfe, et al

- Web Security Sourcebook by Avi Rubin, Dan Geer, and Marcus Ranum
- Web Security & Commerce by Simson Garfinkel with Gene Spafford

Some good security mailing lists

Send your subscription to the email address listed for each group, usualy with a "subscribe listname" in the body of the message.

- Best Security List (bos) best-of-security-request@cyber.com.au
- Bugtraq Full Disclosure List listserv@securityfocus.com
- CERT Advisories cert-advisory- request@cert.org
- CIAC Advisories (ciac bulletin) Majordomo@rumpole.llnl.gov
- COAST Security Archive coast-request@cs.purdue.edu
- Firewalls Digest (firewall-digest) majordomo@lists.gnac.net
- Firewall Wizards (firewall-wizards) majordomo@nfr.net
- FreeBSD Security issues majordomo@freebsd.org
- Intrusion Detection Systems (ids) majordomo@uow.edu.au
- Linux Security Issues linux-security-reguest@RedHat.com
- Legal Aspects of Computer Crime (lacc) majordomo@suburbia.net
- NT Bugtraq listserv@listserv.ntbugtraq.com
- The RISKS Forum (risks) risks-request@csl.sri.com
- WWW Security (ww-security-new) majordomo@nsmx.rutgers.edu
- The Virus Lists (virus-l & virus) LISTSERV@lehigh.edu
- The SANS Digest subject: "subscribe." info@sans.org
- The SANS NewsBites subject: "NewsBites Subscription" digest@sans.org
- The SANS NT Digest subject: "NT Digest." info@sans.org

STARTING POINTS FOR ANTIVIRUS SOFTWARE

A list of Antivirus Software is:

- Symantec - www.symantec.com (Norton AntiVirus 2000);
- Command Software System - www.commandcom.com (Command AntiVirus 4.57);
- F_Secure www.f-secure.com – (F-Secure Anti-Virus 5);
- Computer Associates www.antivirus.cai.com – (InoculateIT 4.5 Personal Edition;
- McAfee – www.mcafee.com – (McAfee VirusScan 4.04);
- Norman Data Defense – www.norman.com – (Norman Virus Control 4.72);
- Panda Software – www.pandasoftware.com – (Panda Antivirus Platinium);
- Trend Micro – www.antivirus.com – (PC-cillin 6).

NOTES ON INTERNET SECURITY

(by the SANS Institute)

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they learn and find solutions for the challenges they face. SANS was founded in 1989. The core of the Institute includes security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire SANS community. During 2000 and 2001, this core will grow rapidly as the Global Incident Analysis Center (GIAC) and the GIAC Certification programs develop mentors who will help new security practitioners master the basics.

The SANS community creates four types of products

- System and security alerts and news updates
- Special research projects and publications
- In-depth education
- Certification

Many SANS resources, such as news digests and research summaries and award-winning papers and security alerts are free to all who ask. Income from printed publications funds university-based research programs. The Global Incident Analysis Center and special research projects are funded by income from SANS educational programs.

Contact addresses:

SANS Institute
5401 Westbard Ave. Suite 1501
Bethesda, MD 20816
Email for information: sans@sans.org
Email for research programs: sansro@sans.org
Email for vendor programs: exhibits@sans.org
Email for certification programs: giactc@sans.org
Conference Registration phone: +1 720 851 2220

Conference Registration FAX: +1 720 851 2221
Office phone: +1 301 951 0102
Office Fax: +1 301 951 0140

The ten most critical Internet security threats (by SANS Institute Roadmap, 3rd edition, Summer of 2000)

1. BIND weaknesses: nxt, qinv and in.named allow immediate root compromise.
2. Vulnerable CGI programs and application extentions (e.g., ColdFusion) installed on web servers.
3. Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (CalendarManager), and rpc.statd that allow immediate root compromise.
4. RDC security hole in the Microsoft Internet Information Server (IIS).
5. Sendmail buffer overflow weaknesses, pipe attacks and MIMEbo, allow immediate root compromise.
6. sadmind and mountd.
7. Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports 135>139 (445 in Windows2000), or UNIX NFS exports on port 2049, or Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548.
8. User Ids, espacially root/administrator with no passwords or weak passwords.
9. IMAP and POP buffer overflow vulnerabilities or incorrect configuration.
10. Default SNMP community strings set to ‘public’ and ‘private’.

The Ten Worst Security Mistakes Information Technology People Make (by SANS Institute Roadmap, 3rd edition, summer 2000)

1. Connecting systems to the Internet before hardening them (removing unnecessary service and patching necessary ones).
2. Connecting test systems to the Internet with default accounts/passwords.
3. Failing to update systems when security vulnerabilities are found and patches or upgrades are available.
4. Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI (public key infrastructures).

5. Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated.
6. Failing to maintain and test backups.
7. Running unnecessary services, especially ftpd, telnetd, finger, rpc, mail, rservices.
8. Implementing firewalls with rules that allow malicious or dangerous traffic-incoming or outgoing.
9. Failing to implement or update virus detection software.
10. Failing to educate users on what to look for and what to do when they see a potential security problem.

ACRONYMS

AC	Access Control
ACL	Access Control List
BSI	Bundesamt für Sicherheit in der Informationstechnik
C4I	Command, Control, Communication, Computing and Intelligence
CAPI	Cryptographic Application Program Interface
CC	Common Criteria
CESG	Communications-Electronics Security Group
CIS	Communication and Information Systems
COMPUSEC	Computer Security
COMSEC	Communications Security
DAC	Discretionary Access Controls
DMS	Decision-Making System
DSB	Defense Science Board
E3	End-to-End Encryption (E3)
EA	Electronic Attack
EAL	Evaluation Assurance Levels
ElP	Electronic Protection
EmP	Emanations Protection
EW	Electronic Warfare
FW	Firewall;
GIAC	Global Incident Analysis Center
GISA	German Information Security Agency
I&A	Identification and Authentication;
IA	Information Assurance
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
INE	In-line Network Encryption
IS	Information Security.

ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria (Europe's White Book)
IW	Information Warfare
JTC	Joint Technical Committee
KDMC	Keys Distribution and Management Center
LAN	Local Area Network
MAC	Mandatory Access Control.
MLS	Multi-Level Security
NAT	Network Address Translation
NCSC	National Computer Security Centre
NNCSA	Netherlands National Communications Security Agency
NSA	National Security Agency
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RA	Remote Access
S/HTTP	Secure Hyper Text Transport Protocol
S/MIME	Secure Multiparty Internet Mail Extension
SSL	Secure Socket Lear
TCSEC	Trusted Computer Security Evaluation Criteria (Orange Book)
TNI	Trusted Network Interpretation of the Trusted Computer Evaluation Criteria (Red Book)
VPN	Virtual Private Network
WAN	World Area Network

INFORMATION SECURITY IN THE 21ST CENTURY: GLOBAL CONVERGENCE

Swedish-Bulgarian Government IT Security Conference

A Swedish-Bulgarian Government IT Security Conference was held from 18 to 24 September 1999 in the Council of Ministers' Hotel in Bansko, Bulgaria--in the foothills of the Pirin Mountain. Main objective of the conference was to establish and strengthen the scientific contacts and collaboration among Swedish and Bulgarian scientists, researchers, and industry representatives.

The International Organizing Committee was co-chaired by Arne Jernelov from the FRN - Swedish Council for Planning and Coordination of Research, and Eugene Nickolov from the National Laboratory of Computer Virology - Bulgarian Academy of Sciences (NLCV-BAS).

The conference was hosted by the National Laboratory of Computer Virology.

Over fifty Bulgarian and Swedish scientists and users participated in the conference, and thirty-two reviewed papers were presented at eight plenary sessions. Two additional sessions for discussions and the concluding session were focused on scientific and policy management issues related to the basic problems of information security.

The topics covered were compliant with European Union's Fifth Framework Program:

- Information Technology and Science;
- Communication science and Human-Computer Interaction;
- Network Technology, Network Security;
- Software Engineering, Middleware, Groupware;
- Data protection, Storage Technology, Cryptography;
- Electronic Commerce, Payment and Signature;
- Security Systems;
- Identification Systems.

Additionally, representatives of governmental institutions of both countries decided of initiate joint activities in the field of IT security, which without any doubt will contribute to the solution of some of the major problems in this area.

NATIONAL LABORATORY OF COMPUTER VIROLOGY

BULGARIAN ACADEMY OF SCIENCES

Organizational status: The National Laboratory of Computer Virology at the Bulgarian Academy of Sciences is unique scientific organization in Bulgaria, specialized in the domain of computer virology and information security.

Subject of research: Computer virology as an independent scientific branch is founded on the achievements of several fundamental scientific branches such as mathematics, computer science, physics, chemistry, and, lately, biology of cell bodies and genetics of microorganisms. The devising of computer viruses is a creative human activity. It has originated almost simultaneously with the creation of the first computer program. And as it often occurs with the human achievements, this idea found its "negative" realization in the information destruction in the millions of computers all over the world. Companies worldwide, each having a judgment on the computer world, make considerable investments in the competition *viruses vs. anti-viruses*, because the outcome of this competition will define to a great extent the future of the computer systems. In particular, this was a typical activity for the past few years when the idea of the biological behavior of the computer viruses and genetically borrowed mechanisms for propagation became a reality and when the self-encoding and self-mutating algorithms of the computer viruses followed closely the model of biological cells and organisms.

Main research areas: Computer Security; Communications Security; Data Security.

Priorities:

- Investigation and classification of new viruses;
- Methods and means for discovery of computer viruses;
- Methods and means for removing computer viruses;
- Methods and means for data recovery;
- Approbation of methods and means listed above;
- Studies in the domain of encryption standards;
- Investigations in the field of the systems for access control;

- Investigations in the domain of client-server applications.

Investigation methods:

- Evaluation of the influence of operational environments - definitions and parameters;
- Evaluation of a given class of computer viruses - definitions and parameters;
- Creation of analytical models - simplification and verification;
- Optimization processes - function, parameters and experiments;
- Creation of simulation models - simplification and verification;
- Analysis of achievements, conclusions, recommendations, corrections;
- Algorithmic solutions for a given class of virus signatures;
- Program realizations for a given class of virus signatures;
- Creation of programs included in the product NLAB;
- Monthly versions for the updating of NLAB.

Main achievements: Compact programs are created for certain platforms, identify more than 50 000 virus signatures and remove the viruses. Effective protections of the type "monitor" and "checker" are created, assuring minimal loss of resources.

Subject of the research of the departments of NLCV:

1. *Department of Computer Security:* Methods and means for discovering and removing computer viruses in computers and computer systems with various operational systems and platforms.
2. *Department of Communications Security:* Methods and means for network protection from computer viruses in computers and computer systems with various operational systems and platforms.

International collaboration: The Laboratory plays an active role in the initiatives and the projects of ACM (Association for Computer Machinery), CARO (Computer Anti-virus Researcher's Organization), EICAR (European Institute for Computer Anti-virus Research), IEEE/CS (IEEE's Computer Society), ISSA (Information Systems Security Association). An active part is also taken in electronic conferences on anti virus topics in the following networks: INet, InterNet, JANet, OMNet, UUNet, VIRNet etc. The Laboratory is a member of the worldwide union of the developers of anti-virus software – Anti-Virus Products Developers. Through the International Federation of Information Processing (IFIP) personal contacts are made and official correspondence exchanged with different technical committees and work groups, for example: IFIP/TC11/WC11.1 Security Management, IFIP/TC11/WG11.3 Database Security, IFIP/TC/WC11.5 System Integrity and Control, IFIP/TC11/ WC11.8 Computer Security Education. Leading young specialists from NLCV

undertake business trips, specialization courses and work in the USA, Canada, Belgium, Japan, Sweden, Denmark, Iceland and other countries.

Education and training: NLCV takes an active part in the training of highly qualified scientists, researchers and staff. In the past years, few dozens of graduation papers were prepared in the Laboratory and submitted successfully in fulfillment of graduation requirements. A series of post-graduate works by external orders were carried out. Few submissions of Ph.D. dissertations are forthcoming. Specialists from the Laboratory lecture and carry on practical sessions on Computer Virology, Computer Security, Communications Security, Data Protection, Computer Network and Systems and Operating Systems in the Sofia University "St. Climent Ohridksi", the Technical University of Sofia, the University for National and World Economy in Sofia, the New Bulgarian University, Burgas, and the Free University. Courses on "Methods and Means for Computer Protection" are organized together with staff from the Parliament, the Presidency, the Ministry of Defense, the Ministry of Finance, the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Transportation and Communications, the National Electric Company and other governmental organizations, as well as for private companies.

RESEARCH AND DEMONSTRATION CENTRE of the Institute for Advanced Defence Research

During the year 2000 a team of IT researchers form the Institute for Advanced Defence Research designed and launched Research and Demonstration Centre (RDC). Main areas of activity of RDC are as follows:

- Installation, investigation and evaluation of hi-tech achievements in the area of information and communications technologies for the needs of the Ministry of Defence and the national security of the Republic of Bulgaria;
- Demonstration of technical and system capabilities;
- Design of pilot projects and evaluation of the technological propositions for C4I system development;
- Education and training.

The tests and expert investigation of the technical solution of the different programmes of the MoD will be completed in accordance with a new model of the life cycle of C4I systems for the Bulgarian armed forces.

The Research and Demonstration Centre will be one of the points of formal contacts between research and teaching staff of the Bulgarian armed forces and the most developed world leaders in area of communications and information technologies.

RDC has the following structure:

- research-demonstration hall with investigation area and site for presentations, press-conferences and lectures;
- Internet laboratory;
- Net–technology and information security laboratory;
- Electronic systems and means laboratory;
- Spectral measurement laboratory;
- Area for business contacts.